单台防火墙双出口组网NAT会话切换异常

NAT 保存上一跳 NAT444 **姚轶群** 2022-02-28 发表

问题描述

单台防火墙双出口双运营商链路，两个接口在同一个安全域，当一条链路断掉后，会话表不会更新，导致下联业务上网不正常，必须要清除会话表才能重新建立会话。

解决方法

解决方法：1、将出接口加入不同的安全域，创建两条nat转换策略，切换链路时就会新建会话

或者开启

2、开启主备链路切换后的NAT会话重建功能

1. 功能简介

广域网双出口组网环境中，分别在NAT设备的出接口（假设为Interface A和Interface B）下配置出方向动态地址转换（引用不同的地址组），基于出接口所属安全域的不同情况，NAT设备的处理机制有所不同：

· 如果两个出接口属于不同的安全域，当Interface A的链路发生故障切换到Interface B的链路时，NAT设备会删除原来的会话表项，由流量触发重新建立NAT会话，保证用户访问外网的业务不受影响。

· 如果两个出接口属于相同的安全域，当Interface A的链路发生故障切换到Interface B的链路时，NAT设备不会删除原来的会话表项，流量与原来的会话表项匹配，导致用户无法访问外网。为了避免该问题的发生，请开启本功能，保证用户业务的可用性。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启主备链路切换后的NAT会话重建功能。

nat link-switch recreate-session

缺省情况下，主备链路切换后的NAT会话重建功能处于关闭状态。